

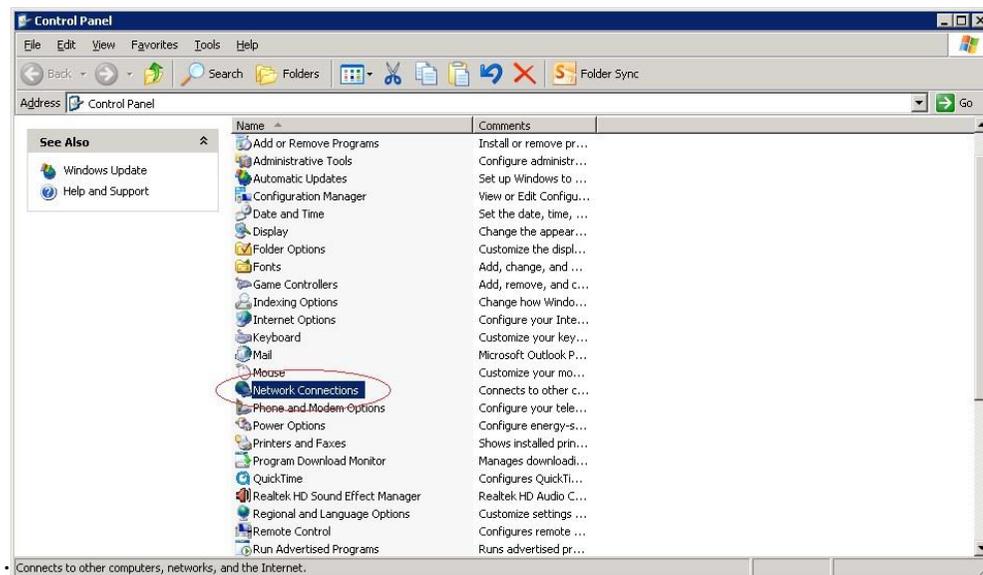
# Network Connectivity Guide

This document contains network connectivity guide to test FAST udp multicast services over Internet VPN sessions. Production connections are available only in dedicated networks and do not use VPN.

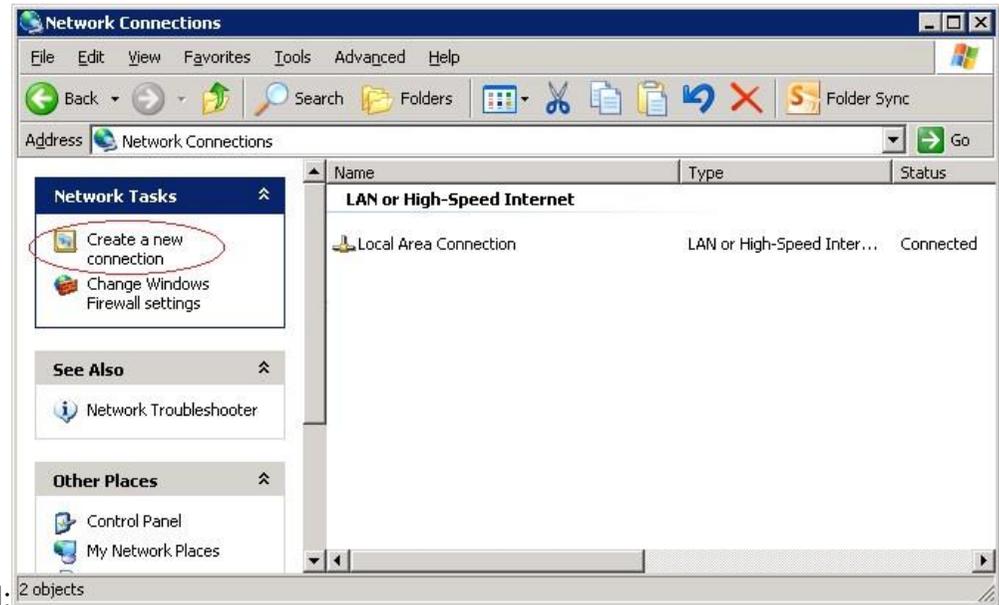
## 1.1. Configure a VPN connection with MOEX using Windows XP

To configure a VPN connection, do the following:

1. Make sure you are connected to the Internet;
2. Click *Start*, and then click *Control Panel*;



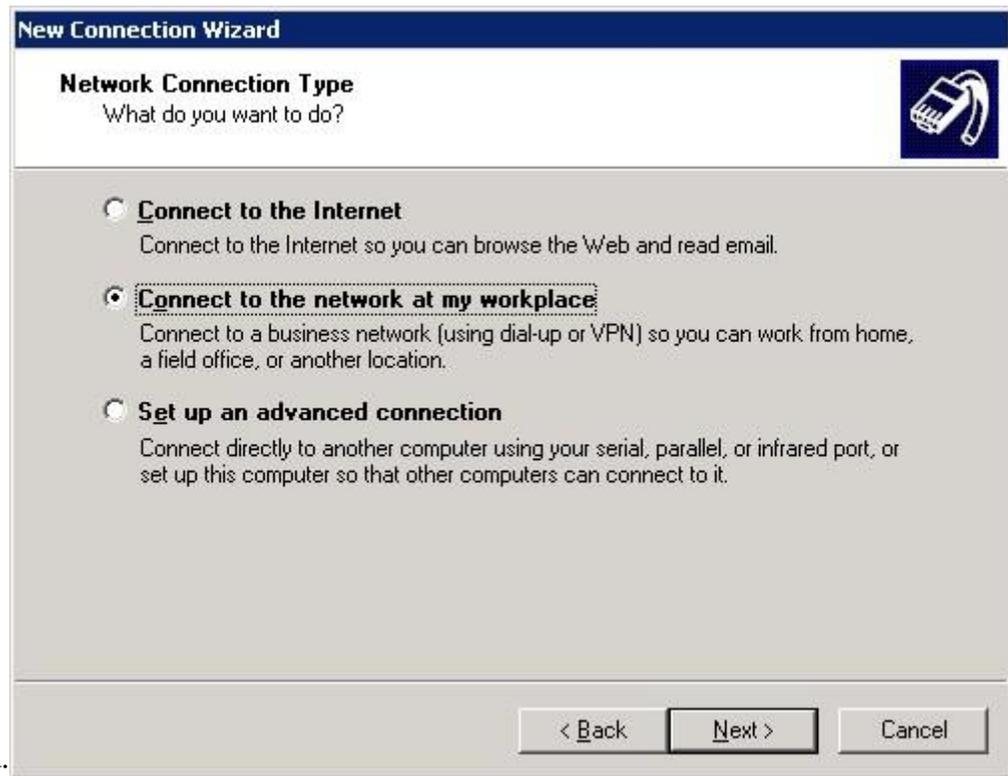
3. In *Control Panel*, double click *Network Connections*:



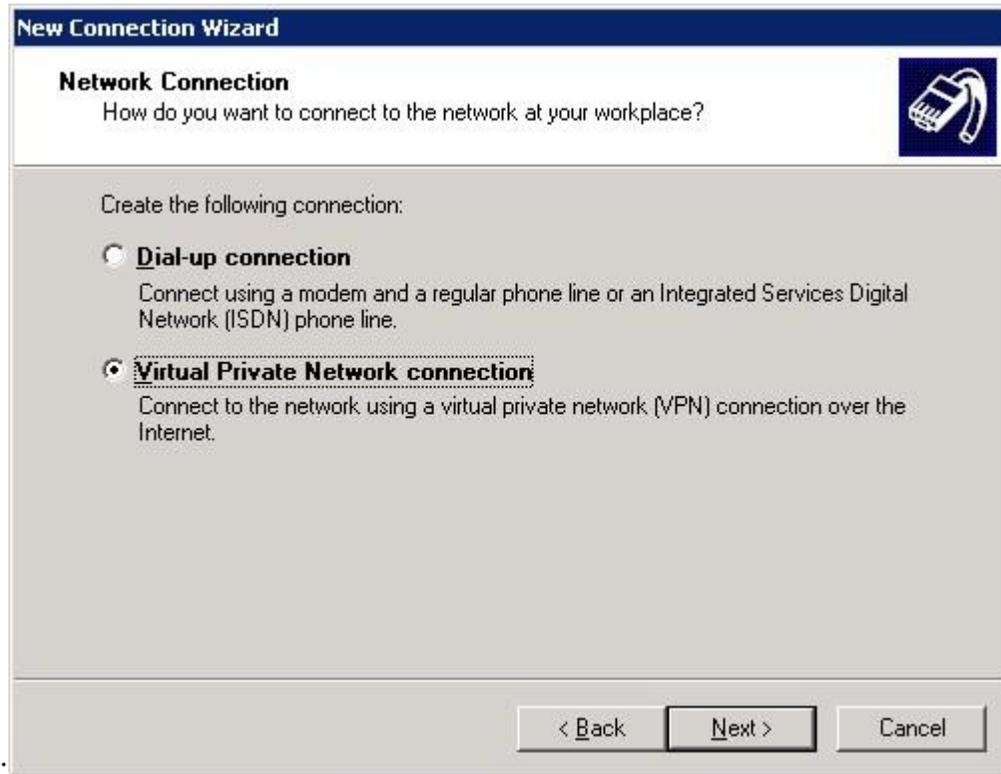
4. Click *Create a new connection* in the *Network Tasks* task pad:



5. In the *Network Connection Wizard*, click *Next*:



6. Click *Connect to the network at my workplace* and then *Next*:



7. Click *Virtual Private Network* connection and then *Next*:
8. Type *Company Name* (e.g. MOEX VPN Connection), and then click *Next*:

**New Connection Wizard**

**Connection Name**  
Specify a name for this connection to your workplace.



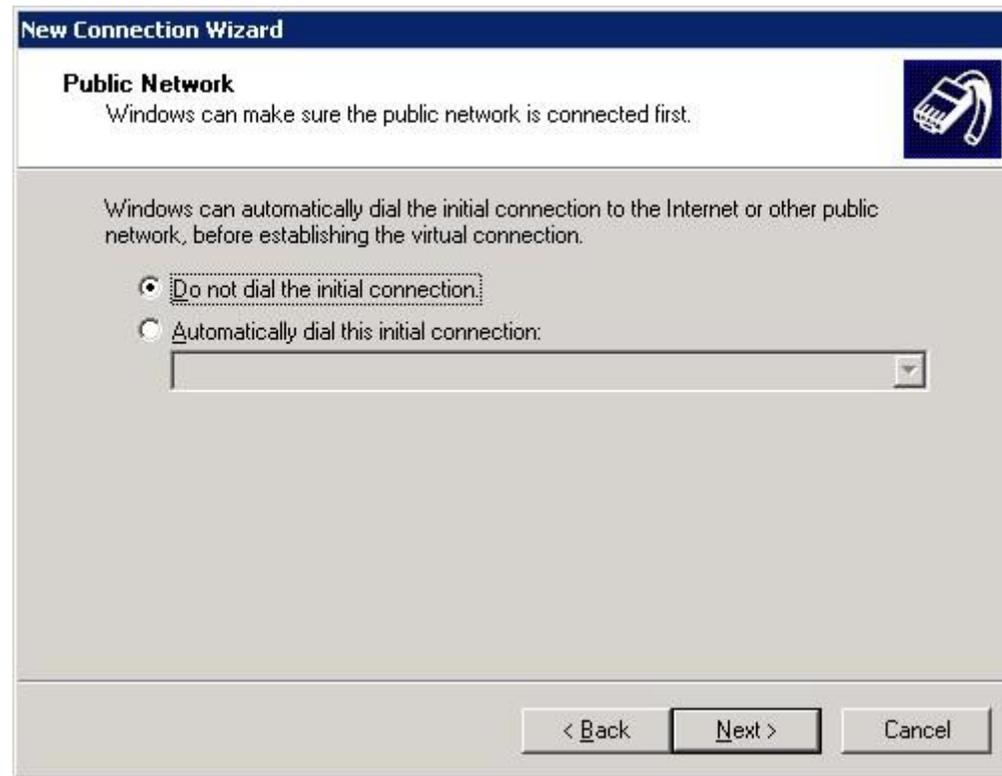
Type a name for this connection in the following box.

Company Name

For example, you could type the name of your workplace or the name of a server you will connect to.

< Back   Next >   Cancel

9. Click *Do not dial the initial connection*, and then click *Next*:



10. Type the server address provided by MOEX team, and then click *Next*:

## New Connection Wizard

### VPN Server Selection

What is the name or address of the VPN server?



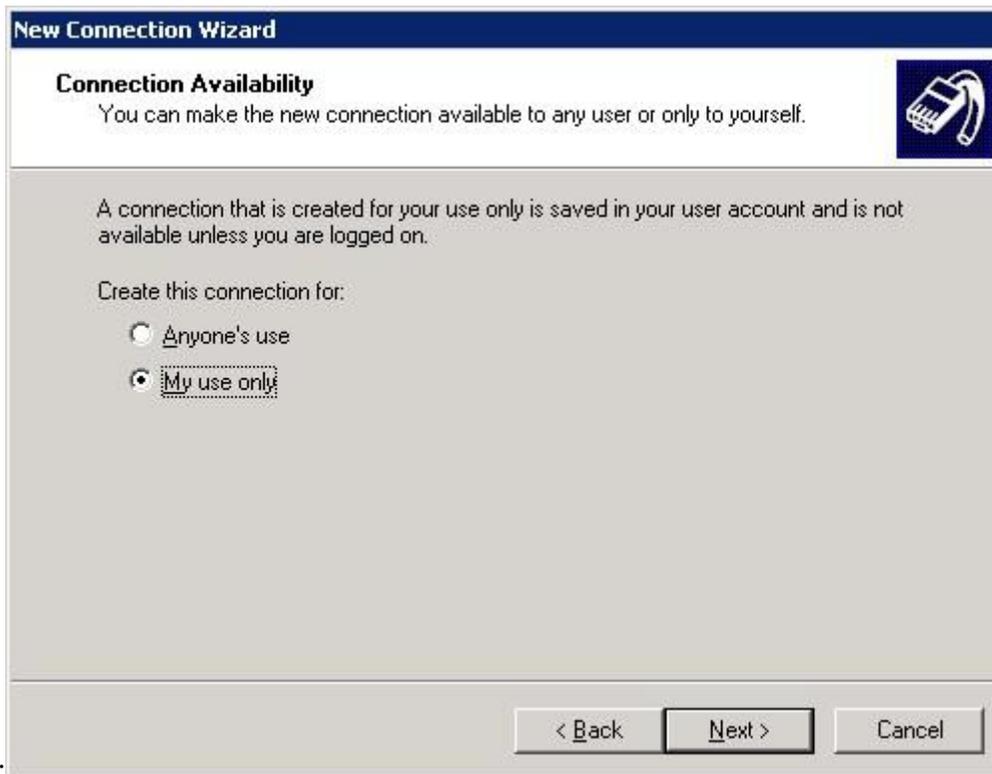
Type the host name or Internet Protocol (IP) address of the computer to which you are connecting.

Host name or IP address (for example, microsoft.com or 157.54.0.1):

< Back

Next >

Cancel



11. Click *My use only* and then *Next*:



12. Click *Finish*:

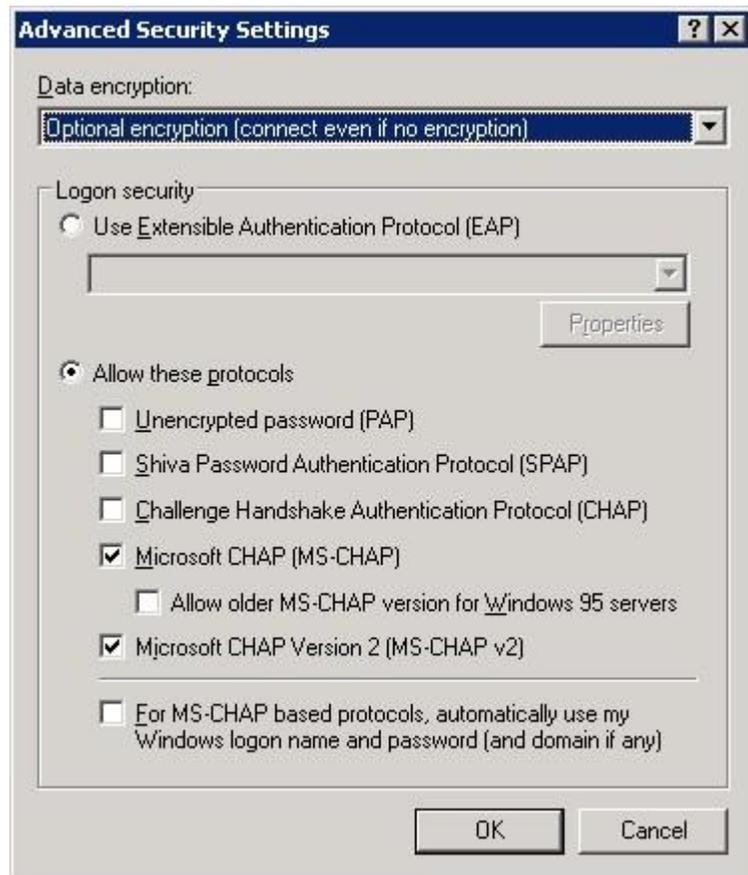


13. Leave *User name* and *Passwod* empty, and then click *Properties*.

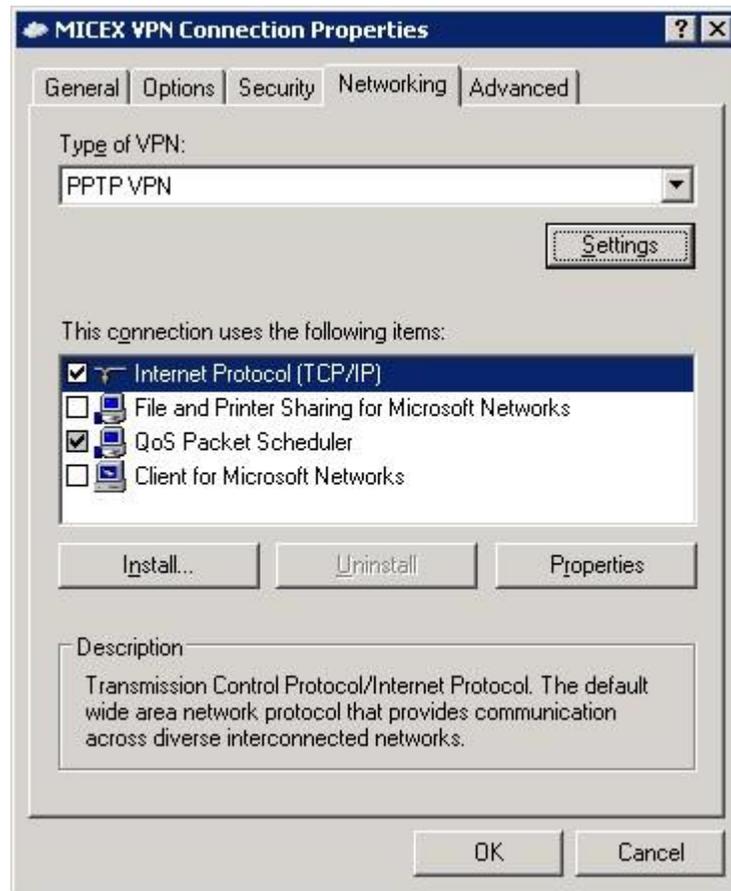
14. On *Security* tab, click *Advanced (custom settings)* and then *Settings...*:



15. Choose *Optional encryption (connect even if no encryption)* data encryption and then click *OK*:

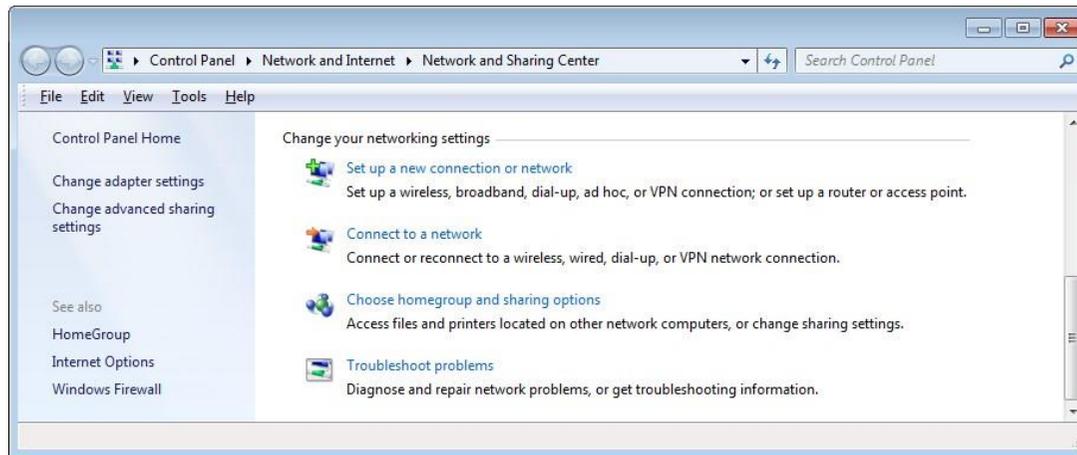


16. On *Networking* tab, choose *PPTP VPN* type of VPN and then click *OK*:

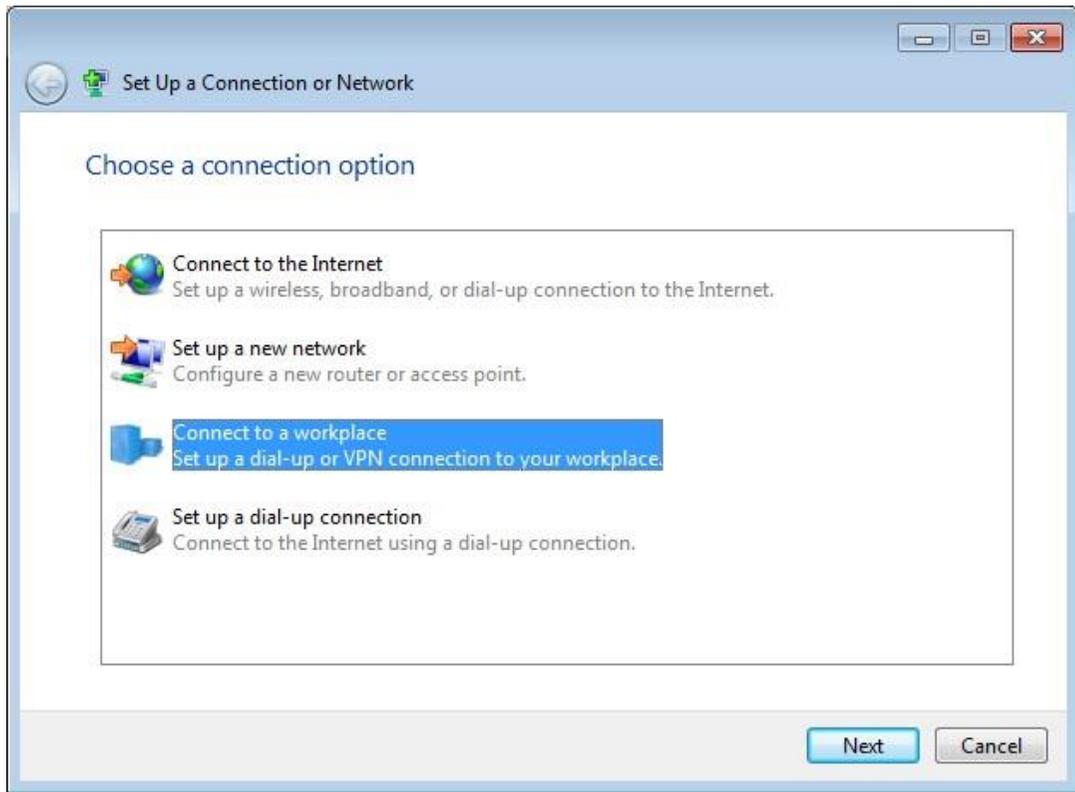


## 1.2. Configure a VPN connection with MOEX using Windows 7

1. Make sure you are connected to the Internet
2. Open *Control Panel*→*Network and Internet*→*Network and Share Center* and then click *Set up a new connection or network*:



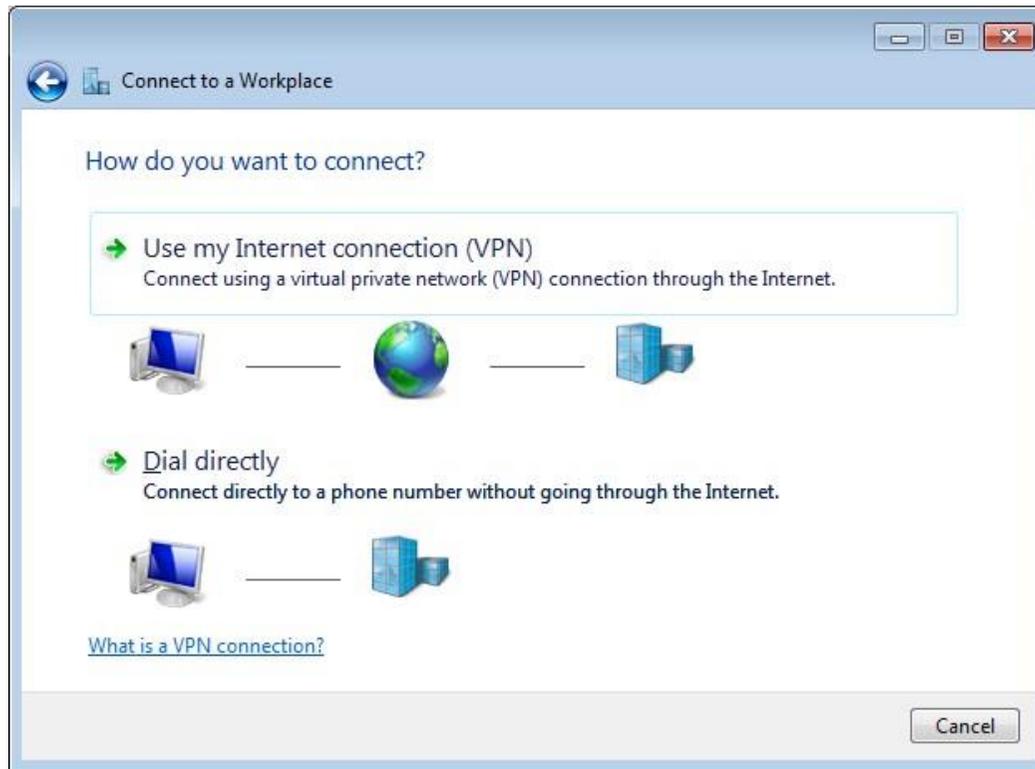
3. Choose *Connect to a workplace* and then click *OK*:





4. Choose *No, create a new connection* and then click *Next*

5. Click *Use my Internet Connection (VPN)*:



6. Type the server address provided by MOEX team to the *Internet address* field, type MOEX VPN Connection to the *Destination name* field, check *Don't connect now; just set it up so I can connect later* and then click *Next*:



7. Leave the next page without changes and then click *Next*:

Connect to a Workplace

Type your user name and password

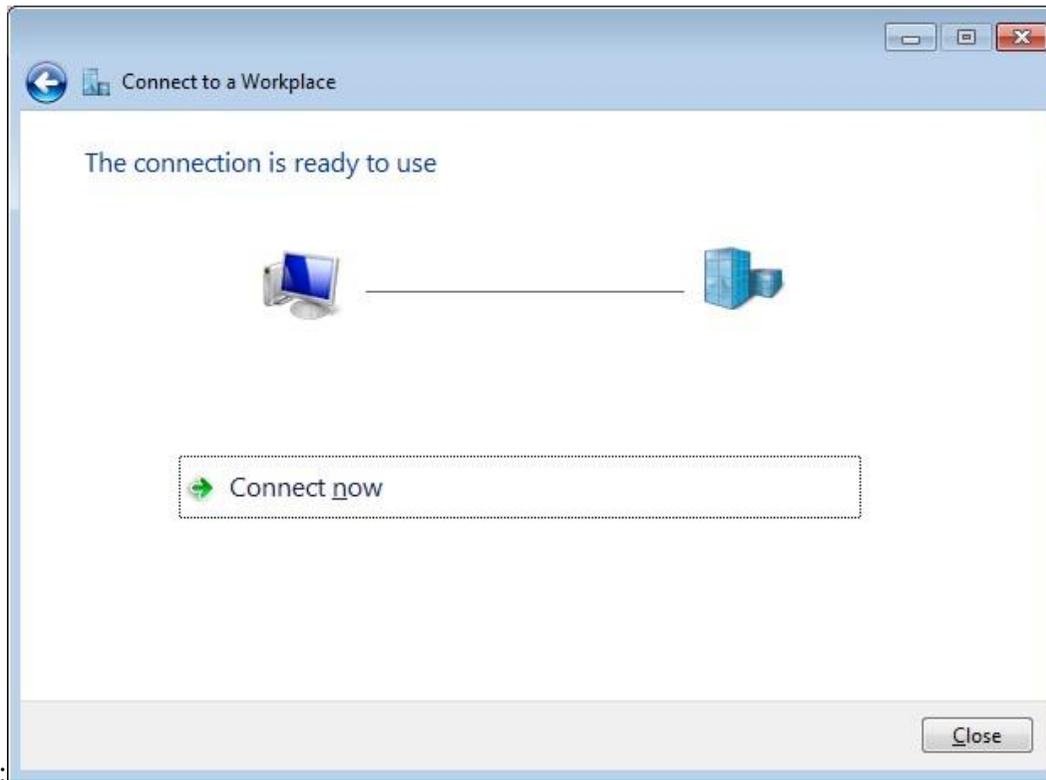
User name:

Password:

Show characters

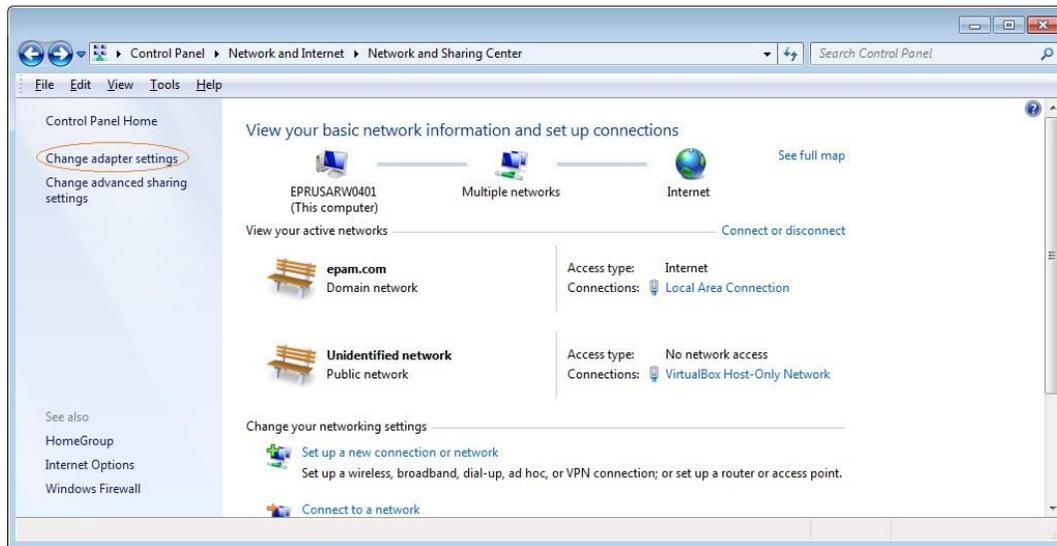
Remember this password

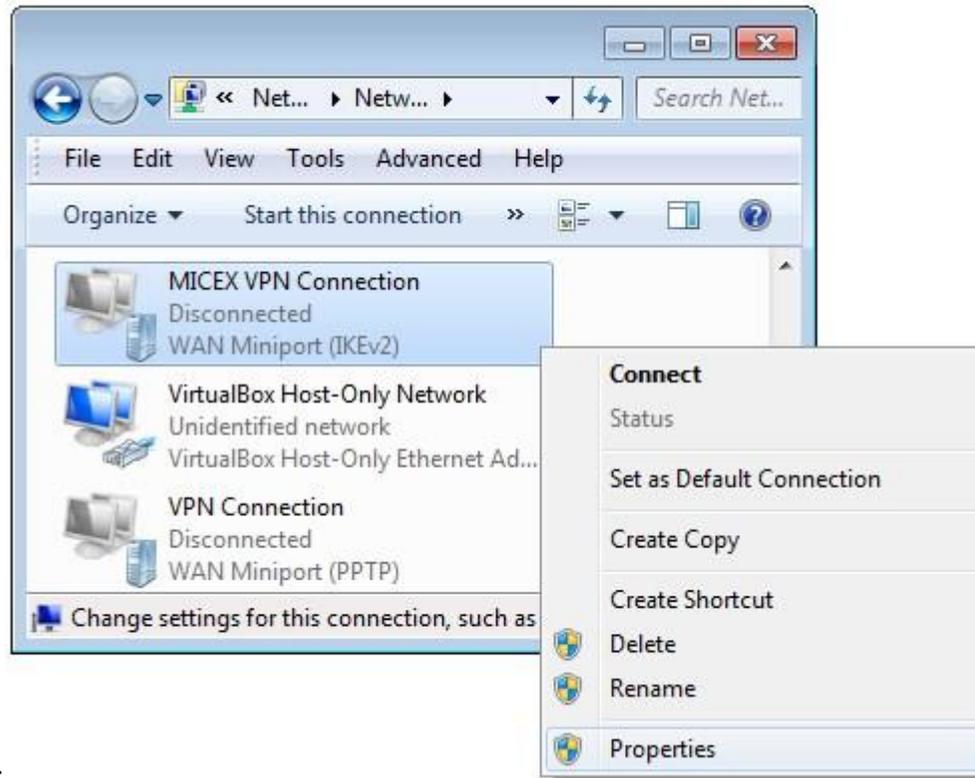
Domain (optional):



8. Click *Close*:

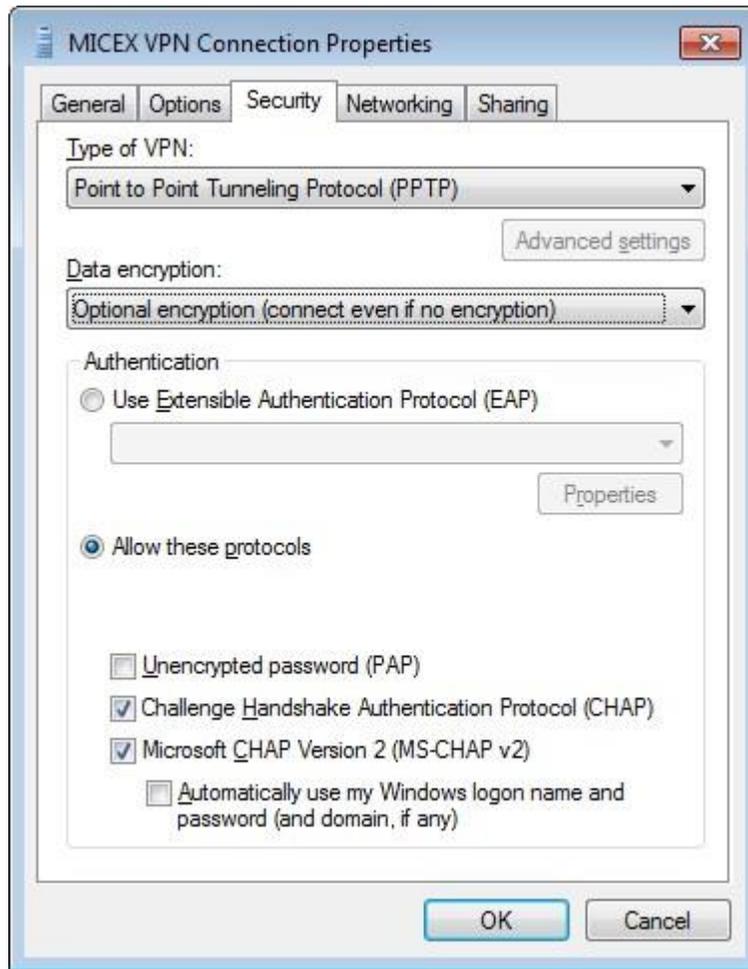
9. Open *Control Panel*→*Network and Internet*→*Network and Share Center* and click *Change adapter setting*:





10. Choose *Properties* of the just created connection:

11. On *Security* tab choose *Point to Point Tunneling Protocol (PPTP)* VPN type, choose *Optional encryption (connect even if no encryption)* data encryption and then click *OK*:



### 1.3. Configure a VPN connection with MOEX using OpenSUSE

1. Make sure you are connected to the Internet;
2. Install *pptp* client using the following command:

```
sudo zypper install pptp
```

3. Run the following command:

```
sudo /usr/sbin/pptp-command setup
```

4. Type '4' and press enter:

```
1.) Manage CHAP secrets
2.) Manage PAP secrets
3.) List PPTP Tunnels
4.) Add a NEW PPTP Tunnel 5.)
Delete a PPTP Tunnel
6.) Configure resolv.conf
7.) Select a default tunnel
8.) Quit
?: 4 + <enter>
```

5. Type '1' and press enter:

```
Add a NEW PPTP Tunnel.
```

```
1.) Other
Which configuration would you like to use?: 1 + <enter>
```

6. Type 'micex\_vpn\_connection' and press enter:

```
Tunnel Name: micex_vpn_connection + <enter>
```

7. Type '<server address>' and press enter:

```
Server IP: <server address> + <enter>
```

8. Type 'del default' and press enter:

```
route: del default + <enter>
```

9. Type 'add default gw 1.1.1.1 TUNNEL\_DEV' and press enter: `route: add default gw 1.1.1.1 TUNNEL_DEV`

10. Simply press enter:

```
route: <enter>
```

11. Type 'test' and press enter:

```
Local Name: test
```

12. Leave a default value, simply press enter: Remote Name [PPTP]: <enter>

13. If you have done everything correct, you will see:

```
Adding micex_vpn_connection - <server address> - test - PPTP  
Added tunnel micex_vpn_connection
```

14. Type 'q' and press enter to exit the setup wizard.

15. The next step is to make a few changes in a configuration file which was created on previous steps by the wizard. At first open it using the following command:

```
sudo vim /etc/ppp/peers/micex_vpn_connection
```

16. Needed changes are colored by red:

```
#
```

```
# PPTP Tunnel configuration for tunnel micex_vpn_connection
# Server IP: <server address>
# Route: route del default
# Route: route add default gw 1.1.1.1 TUNNEL_DEV
#
noauth
#
# Tags for CHAP secret selection
# name test
remotename PPTP

#
# Include the main PPTP configuration file
#
# file /etc/ppp/options.pptp
```

17. Please be careful and don't forget to save this file before closing. That's all. Now you are ready to establish the VPN connection using the following command:

```
sudo /usr/sbin/pptp-command start micex_vpn_connection
```

You will see something like this:

```
Using interface ppp0 Connect:
ppp0 <--> /dev/pts/1 local
IP address 1.1.1.19 remote IP
address 1.1.1.1
Script ?? finished (pid 30023), status = 0x0
Script /etc/ppp/ip-up finished (pid 30032), status = 0x0
Route: add -net 0.0.0.0 gw 1.1.1.1 added
Route: add -net 1.1.1.0 netmask 255.255.255.0 gw 1.1.1.1 added
All routes added.
Tunnel micex_vpn_connection is active on ppp0. IP Address: 1.1.1.19
```

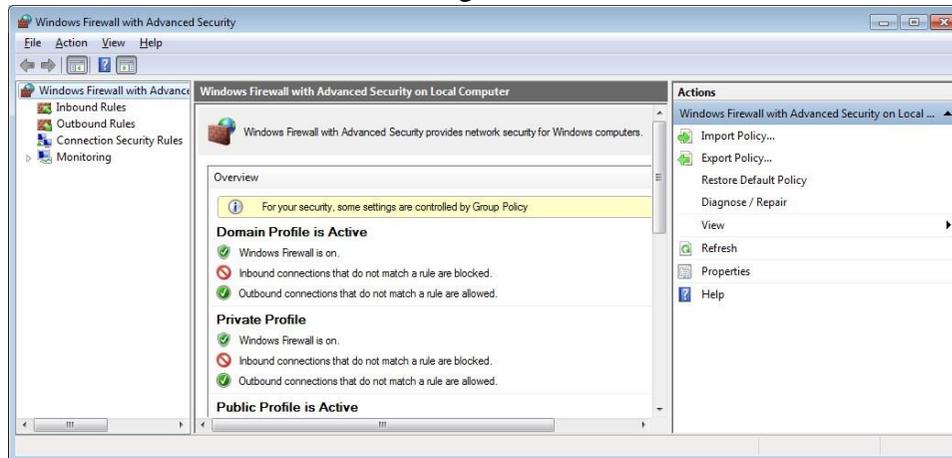
18. To stop this connection use the following command:

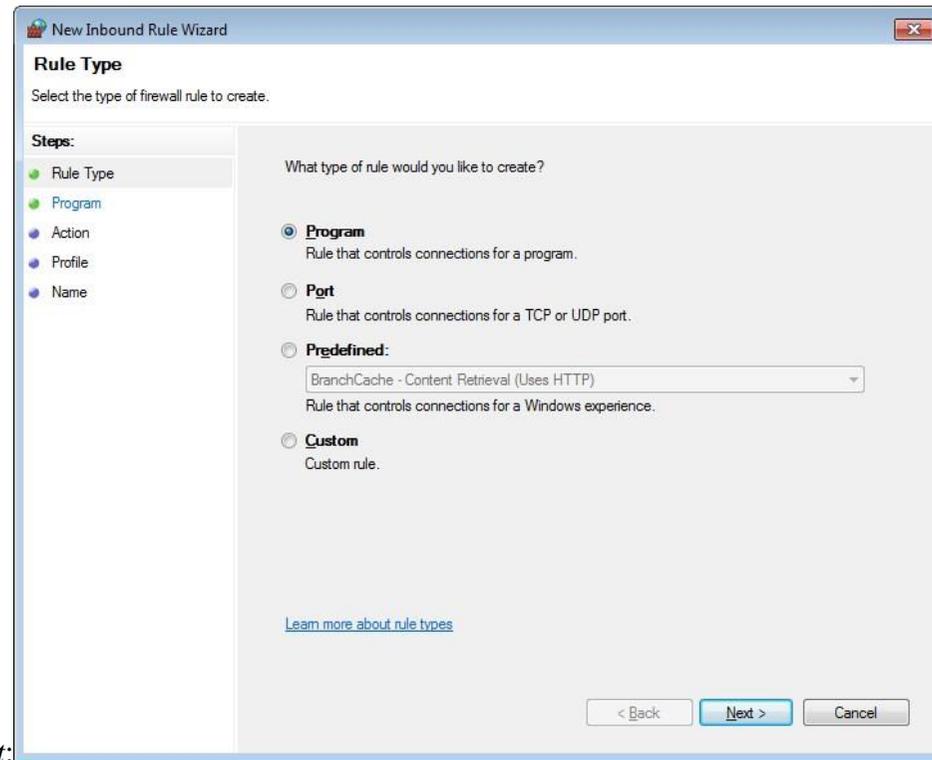
```
sudo /usr/sbin/pptp-command stop
```

19. Important: After the VPN connection is stopped you will need to return the default route rule you had before. Otherwise the next tries to establish the VPN connection will be failed. It's recommended to make a script which will be responsible for the default route rule restoring.

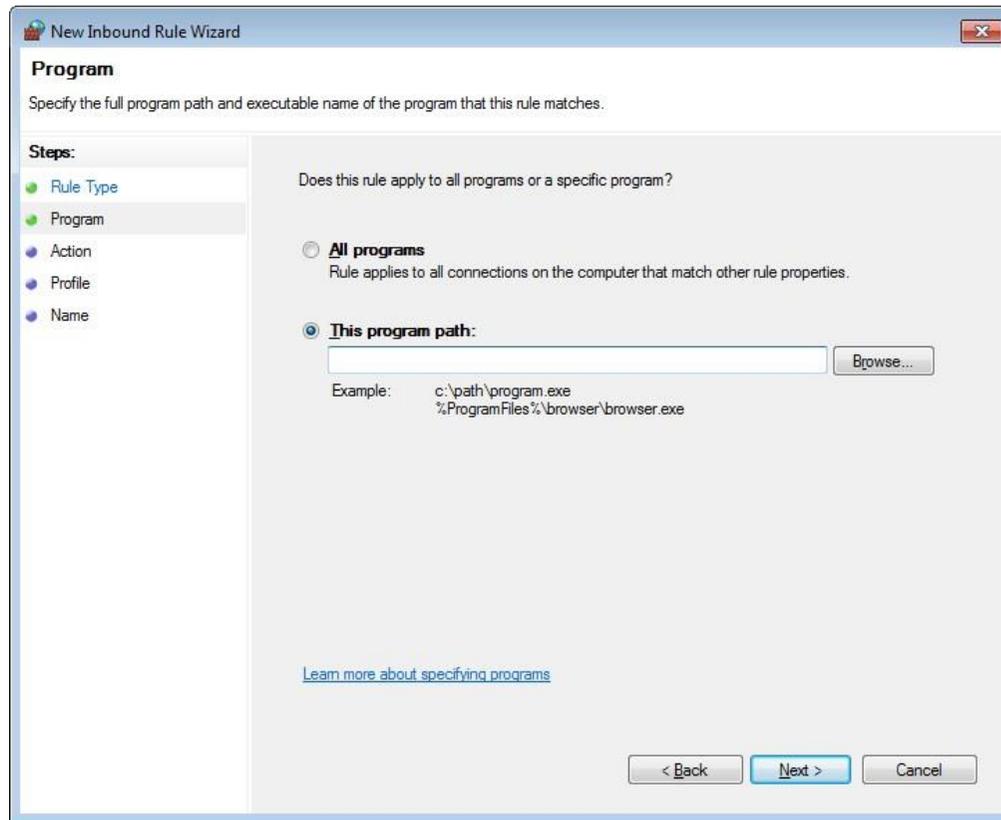
## 1.4.Troubleshooting

1. The VPN connection is established but your application doesn't receive UDP packets (Windows 7)
  - 1.1 Open status of your VPN connection and check if the count of 'Received' bytes is continuously growing; If it's not so, ask for help the MOEX support team.
  - 1.2 Check firewall settings. Temporary turn off the firewall. If after that all seems ok, turn on firewall again but add the firewall rule:
    - ✓ Open *Windows Firewall*→*Advanced* settings;
    - ✓ Choose *Inbound Rules* and on the right click *New Rule*:





- ✓ Leave the first page without changes and click *Next*:
- ✓ On the next page you need to specify path to your program:



✓ Leave the pages below without changes:

New Inbound Rule Wizard

**Action**

Specify the action to be taken when a connection matches the conditions specified in the rule.

**Steps:**

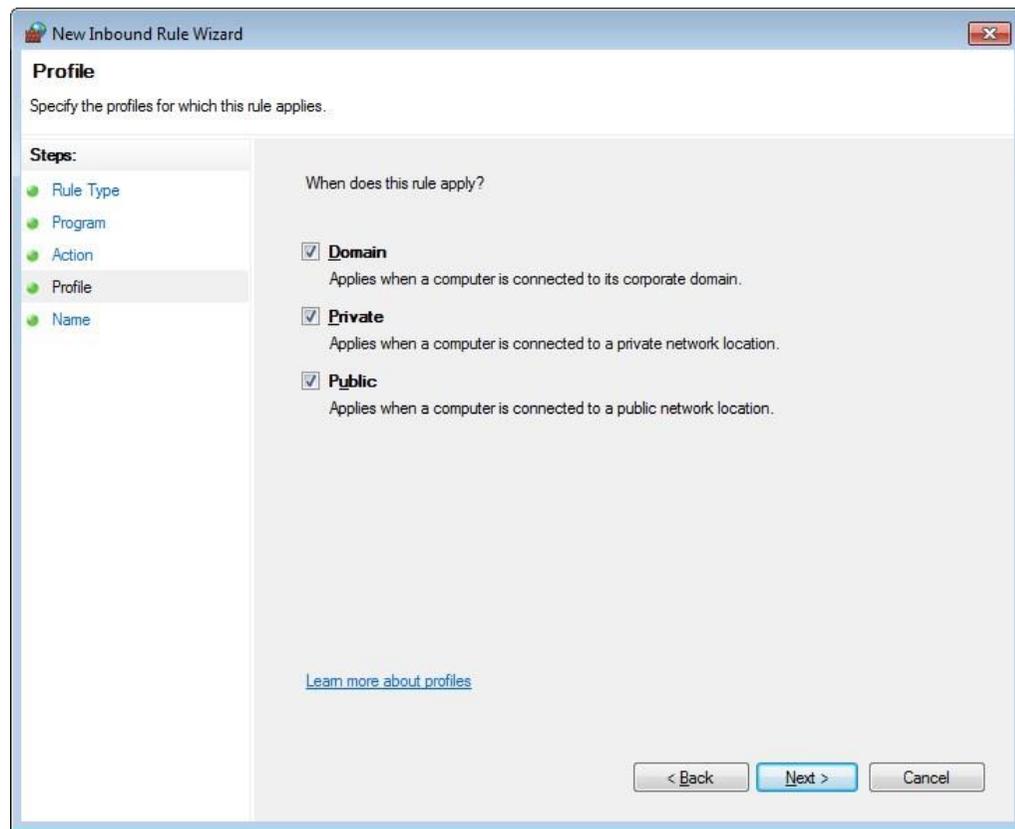
- Rule Type
- Program
- Action**
- Profile
- Name

What action should be taken when a connection matches the specified conditions?

- Allow the connection**  
This includes connections that are protected with IPsec as well as those are not.
- Allow the connection if it is secure**  
This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.
- Block the connection**

[Learn more about actions](#)

< Back   Next >   Cancel



- ✓ Here you should to specify the name of this rule. E.g. MyApplicationRule.

New Inbound Rule Wizard

**Name**

Specify the name and description of this rule.

**Steps:**

- Rule Type
- Program
- Action
- Profile
- Name

Name:

Description (optional):

< Back Finish Cancel